UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/672,811	09/26/2003	Tom Thuan Cheung	SVL920030076US1	8922

28342 7590 05/31/2007

SAMUEL A. KASSATLY LAW OFFICE
20690 VIEW OAKS WAY
SAN JOSE, CA 95120

EXAMINER	
SHAN, APRIL YING	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
05/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/672,811	CHEUNG, TOM THUAN	
	Examiner	Art Unit	
	April Y. Shan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 March 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,8-10 and 12-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8-10 and 12-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. The Applicant's amendment, filed 19 March 2007, has been received, entered into the record, and respectfully and fully considered.

2. As a result of the amendment, claims 1-3, 8 and 15-20 have been amended. Claims 7 and 11 are cancelled. Claims 1-6, 8-10 and 12-20 are now presented for examination.

3. Any objections/rejections not repeated below for record are withdrawn due to Applicant's amendment.

4. The examiner is aware of that the Applicant replaced "transforms" with "maps" in some of the claims. According to Oxford English Dictionary Online http://dictionary.oed.com/entrance.dtl, (Oxford University Press 2007) defines "map" on page 3, as "To be associated with or transformed into by a mapping". The Applicant is respectfully reminded that although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993)

Claim Objections

5. Claims 1-6, 8-10 and 12-20 are objected to because of the following informalities:

As per **claim 1**, the preamble recites "...method of **encrypting**". However, the body of the claim only recites "**defining** an encryption equation that maps....". Further, the body of the claim recites "**decrypting**...". Is this the Applicant's intention to claim a method of decryption instead? Further, "presenting the decrypting original string for

processing" should be "presenting the decrypted original string for processing". Furthermore, "a processor-implemented method..." in claim 1 is not clearly defined/supported in the original disclosure. Applicant is required to point out where this amended claim limitation is in the original disclosure and please note no new matter should be added in the original disclosure in addressing this claim objection. Also, the step of encrypting the original string is critical or essential to the practice of the invention, but not included in the claim(s) and the step of determine factor decryption equations is critical or essential to the practice of the invention, but not included in the claim(s).

Any claim not specifically addressed, above, is being rejected as incorporating the deficiencies of a claim upon which it depends.

As per **claims 15 and 18**, the preamble recites "...system/computer program product for **encrypting and decrypting**". However, the body of the claim only recites "**defining** an encryption equation that maps...". Where is encrypting? Is this the Applicant's intention to claim a system/computer program product of decryption instead? Further, "presenting the decrypting original string for processing" should be "presenting the decrypted original string for processing". Furthermore, "a processor-implemented system..." in claim 15 is not clearly defined/supported in the original disclosure. Applicant is required to point out where this amended claim limitation is in the original disclosure and please note no new matter should be added in the original disclosure in addressing this claim objection. Also, the step of encrypting the original string is critical or essential to the practice of the invention, but not included in the

claim(s) and the step of determine factor decryption equations is critical or essential to the practice of the invention, but not included in the claim(s).

Any claim not specifically addressed, above, is being objected as incorporating the deficiencies of a claim upon which it depends.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 1-6, 8-10 and 12-20 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

As per claims 1, 15 and 18, they recite "**decrypting the original string** using the **derivative equations** and factors and presenting the **decrypting original string** for processing". However, in par. [0035] of the Applicant's original disclosure, the Applicant discloses "...A decryption module 240 decrypts output 225 to produce a decrypted string 245...The decrypted string 245 is equal to the original string 215". Clearly, the claims as recited are contradicted to the original disclosure, which is not enabling. How to decrypt an original string, which is not encrypted and why to decrypt an original string, which is not encrypted? Additionally, in par. [0053] and block 535 in fig. 5B, the

Applicant discloses, "The decryption module 240 decrypts the encrypted character at block 535 (Fig. 5B) using factors 220 and the **decryption equation**". If using derivative equations as claimed to decrypt, then why in the previous step, to "determining a decryption equation..." Further, in par. [0045] and [0046] of the Applicant's original disclosure, the Applicant discloses, "...at block 320, obtaining **the factor decryption equations** that map derivatives 230 to factors 220...to obtain the **decryption equation** (block 325). Clearly, the factor decryption equations that map derivatives are not the decryption equation as claimed. Furthermore, the Applicant recites, "selectively defining a set of derivatives **relating** to the factors, wherein the set of derivatives contain a plurality of false derivatives that are not used to decrypt the encrypted string". But according to Applicant's original disclosure par. [0034], the Applicant discloses "additional derivatives may be provided that are **not actually used to determine the factors**; the presence of these false derivatives provide an additional level of security in the encryption method of system 10". Clearly, the newly added claim limitation is contradicted with the disclosure, which is not enabling. So, the false derivatives must not be included in the defined set of derivatives since the defined set of derivatives according to the claim relating to the factors. *In re Wands, 858 F. 2d 731, 737, 8 USPQ2d 1400, 1404 (Fed. Cir. 1998).*

Any claim not specifically addressed, above, is being rejected as incorporating the deficiencies of a claim upon which it depends.

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 1-6, 8-10 and 12-20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claims 1, 15 and 18, they recite, "**decrypting the original string** using the **derivative equations** and factors and presenting the **decrypting original string** for processing". However, in par. [0035] of the Applicant's original disclosure, the Applicant discloses "...A decryption module 240 decrypts output 225 to produce a decrypted string 245...The decrypted string 245 is equal to the original string 215". Clearly, the claims as recited are contradicted to the original disclosure. How to decrypt an original string, which is not encrypted and why to decrypt an original string, which is not encrypted? Further, in par. [0053] and block 535 in fig. 5B, the Applicant discloses, "The decryption module 240 decrypts the encrypted character at block 535 (Fig. 5B) using factors 220 and the **decryption equation**". If using derivative equations as claimed to decrypt, then why in the previous step, to "determining a decryption equation..." Furthermore, in par. [0045] and [0046] of the Applicant's original disclosure, the Applicant discloses, "...at block 320, obtaining **the factor decryption equations** that map derivatives 230 to factors 220...to obtain the **decryption equation** (block 325). Clearly, the factor decryption equations that map derivatives are not the decryption equation as claimed. Finally, Furthermore, the Applicant recites, "selectively defining a set of derivatives **relating** to the factors, wherein the set of derivatives contain a plurality of false derivatives that are not used to decrypt the encrypted string". But according to Applicant's original disclosure par. [0034], the Applicant discloses

"additional derivatives may be provided that are **not actually used to determine the factors**; the presence of these false derivatives provide an additional level of security in the encryption method of system 10". Thus, this claim limitation is contradicted with itself.

Any claim not specifically addressed, above, is being rejected as incorporating the deficiencies of a claim upon which it depends.

Claim Rejections - 35 USC § 101

10. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

11. Claims 15-20 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 15-17 are directed a system for encrypting and decrypting an original string. However, it appears that the system to one of ordinary skill in the art is software, per se. The Applicant amended the claim by adding "a processor-implemented system...". However, processor-implemented system means the system is **not** currently implementing with the processor, therefore, the system is still software, per se. Further, as stated in the claim objection, the examiner finds "processor-implemented system..." is not defined in the original disclosure and thus, "During patent examination the pending claims must be interpreted as broadly as their terms reasonably allow..." *(See in re Zletz, 893 F.2d 319, 321-22, 13 USPQ2d 1320, 1322 (Fed. Cir. 1989))*. The examiner's position is a processor can be reasonably interpreted by one of ordinary skill in the art as software. According to "The Authoritative Dictionary of IEEE Standards

Terms Seventh EDITION", processor is defined as "(**software**) A computer program that includes the compiling, assembling, translating, and related functions for a specific programming language" on page 872. So, there is no element positively recited as part of the system and it appears that such would reasonably be interpreted as representative of the software which encrypts and decrypts an original string. As such, it believed that the system of claim 15-17 is reasonably interpreted as functional descriptive material, per se.

Claims 18-20 are directed to a computer program product stored on a computer readable storage medium for encrypting and decrypting an original string. The Applicant amended the claim by adding "a computer program product... stored on a computer readable storage medium...". However, a computer program product... stored on a computer readable storage medium means the computer program product is **not** currently storing on a computer readable storage medium, therefore, the computer program product is still software, per se. As such, it believed that the computer program product of claims 18-20 is functional descriptive material, per se.

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

14. Claims 1-6, 8-10 and 12-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brakley, III et al. (U.S. Patent No. 5,677,952).

As per **claims 1 and 15**, Blakley, III et al. discloses a method/system of encrypting (abstract) an original string ("data (i.e., a string x)" – e.g. col. 5, lines 10-11), comprising:

selectively defining a set of factors ("a password Pu and possibly a user name and other usercheck data" – e.g. col. 5, lines 43-44. Please note a password Pu and possibly a user name and other usercheck data correspond to Applicant's factors) that represents factors to be used for encrypting the original string (abstract);

defining an encryption equation ("encryption function 86, usually an XOR" – e.g. col. 5, lines 39-40, col. 6, line 10) that maps the original string to an encrypted string (col. 5, lines 39-40);

selectively defining a set of derivatives relating to the factors ("the secret key is derived from a password entered into the computer by an authorized user", "an index" – e.g. abstract, "To create the "efficient representation" of the secret key, the key is preprocessed into **a table of** pseudorandom values. The index (i.e., the sector

identification) and **a set of values from a table** is then used to generate initial values for a plurality of registers..." – e.g. col. 8, lines 3-24. Please note secret key, index and registers correspond to Applicant's derivatives),

selectively defining a set of derivative equations ("pseudorandom function 84" – e.g. col. 5, line 38. Please note pseudorandom function corresponds to Applicant's derivative equation) that represents relationships between the factors and the derivatives to introduce a predetermined degree of randomness in encrypting the original string (abstract); and

Determining a decryption equation that maps the derivatives to the factors (e.g. col. 6, lines 25-47);

Decrypting (e.g. abstract) the original string ("data (i.e., a string x)" – e.g. col. 5, lines 10-11) using the derivative equations and the factors (e.g. col. 6, lines 25-47); and presenting the decrypting original string for processing (e.g. col. 1, lines 61-63, col. 2, lines 18-19 and col. 10, lines 26-29)

Blakley, III et al. does not expressly disclose wherein the set of derivatives contains a plurality of false derivatives that are not used to decrypt the encrypted string. However, in col. 8, lines 3-24, Blakley, III et al. discloses ""To create the "efficient representation" of the secret key, the key is preprocessed into **a table of** pseudorandom values. The index (i.e., the sector identification) and **a set of values from a table** is then used to generate initial values for a plurality of registers..." and also Blakley, III discloses in the abstract "...applying a length-increasing pseudorandom function to the secret key and an index to generate a pseudorandom bit string..." and "The

pseudorandom bit string is then used to...decrypt data...". From Blakley, III et al.'s teaching, it would have been obvious to a person with ordinary skill in the art at the time of the invention that set of derivatives (a table of pseudorandom values in Blakley, III et al.) contains a plurality of false derivatives that are not used to decrypt the encrypted string (only a set of value from a table is then used to generate initial values for a plurality of registers and the masked register values are then concatenated into the pseudorandom bit string for decryption as disclosed by Blakley, III et al. Therefore, it would have been obvious that other sets of values from a table are false derivatives that are not used to decrypt the encrypted string. The motivation of doing so would have been "to create the "efficient representation" of the secret key" therefore, "it must be impossible for the attacker, who does not know the secret key to distinguish fa(i) from a random function of i" (Brakley, III et al. col. 8, lines 7-9) in order "to protect the confidentiality of information stored on a storage device of a computer, even if the computer is stolen or otherwise access without the owner's consent or knowledge", as taught by Brakley, III et al. (col. 1, lines 44-47)

As per **claim 2**, Blakley, III et al. discloses a method as applied above in claim 1. Blakley, III et al. further discloses wherein the set of factors comprises at least one of: constant values, numbers, objects, and random values that are derived from events ("a password Pu and possibly a user name and other usercheck data" – e.g. col. 5, lines 43-44).

As per **claim 3**, Blakley, III et al. discloses a method as applied above in claim 1. Blakley, III et al. further discloses wherein the set of factors comprises at least one of: constant values, numbers, objects, and random values that are derived from values provided by equations ("a password Pu and possibly a user name and other usercheck data" – e.g. col. 5, lines 43-44.)

As per **claim 4**, Blakley, III et al. discloses a method as applied above in claim 1. Blakley, III et al. further discloses wherein the derivative equations comprise mathematical functions that are defined in terms of the factors ("a= SHA(Pu)+Ku" – e.g. col. 5, lines 3-9)

As per **claim 5**, Blakley, III et al. discloses a method as applied above in claim 1. Blakley, III et al. further discloses wherein the number of the derivative equations is at least equal to the number of the factors ("a length-increasing pseudorandom function and a password" – e.g. abstract).

As per **claim 6**, Blakley, III et al. discloses a method as applied above in claim 1. Blakley, III et al. further discloses wherein the original string is comprised of characters (("data (i.e., a string x)" – e.g. col. 5, lines 10-11. Please note a string is composed of a sequence of characters representing human-readable text. Therefore, Blakley, III et al. met the claim limitation by disclosing a string X).

As per **claim 8**, Blakley, III et al. discloses a method as applied above in claim 1. Blakley, III et al. further discloses comprising determining a plurality of factor decryption equations that map the derivatives to a plurality of mapped factors (col. 6, lines 25-47)..

As per **claim 9**, Blakley, III et al. discloses a method as applied above in claim 8. Blakley, III et al. further discloses comprising determining a decryption equation as a mathematical function of an encrypted string in the encrypted string and the plurality of mapped factors (col. 6, lines 25-47).

As per **claim 10**, Blakley, III et al. discloses a method as applied above in claim 9. Blakley, III et al. further discloses comprising storing the encrypted string in a database with a set of stored derivatives (col. 6, lines 25-33 and lines 48-57).

As per **claim 12**, Blakley, III et al. discloses a method as applied above in claim 1. Blakley, III et al. further discloses comprising decrypting the encrypted string based on the derivatives and the derivative equations (col. 6, lines 25-47).

As per **claim 13**, Blakley, III et al. discloses a method as applied above in claim 1. Blakley, III et al. further discloses wherein selectively defining the set of factors comprises defining at least one factor ("a password Pu and possibly a user name and other usercheck data" – e.g. col. 5, lines 43-44.)

As per **claim 14**, Blakley, III et al. discloses a method as applied above in claim 1. Blakley, III et al. further discloses wherein selectively defining the set of derivative equations comprises defining at least one derivative equation (abstract).

As per **claim 16**, Blakley, III et al. discloses a system as applied above in claim 15. Blakley, III et al. further discloses wherein the set of factors comprises at least one of: constant values, numbers, objects, and random values that are derived from events ("a password Pu and possibly a user name and other usercheck data" – e.g. col. 5, lines 43-44).

As per **claim 17**, Blakley, III et al. discloses a system as applied above in claim 15. Blakley, III et al. further discloses wherein the set of factors comprises at least one of: constant values, numbers, objects, and random values that are derived from values provided by equations ("a password Pu and possibly a user name and other usercheck data" – e.g. col. 5, lines 43-44).

As per **claims 18-20**, Blakley, III et al. discloses the claimed method of steps as applied above in claim 1-3. Therefore, Blakley, III et al. discloses the claimed computer program product having instruction codes for carrying out the method of steps.

Response to Arguments

15. Applicant's arguments with respect to claims 1, 15 and 18 have been considered but are moot in view of the new ground(s) of rejection.

16. The Applicant argues on page 9 of the remark, "...the inclusion of the limitation of claim 11 in the independent claims 1, 15 and 18...", the examiner respectfully points out the amended claims 1, 15 and 18 added "selectively defining a set of derivatives relating to the factors, wherein the set of derivatives contains a plurality of false derivatives that are not used to decrypt the encrypted string" and "determining a decryption equation...decrypting the original string...and presenting the decrypting original string for processing" and the original claim 11 only recites "wherein the set of stored derivatives contains a plurality of false derivatives that will not be used to decrypt the encrypted string".

Conclusion

17. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-892)

18. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to April Y. Shan whose telephone number is (571) 270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AYS
5-23-2007

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100